IBAIS University
ইবাইস ইউনিভার্সিটি

© 2007 Journal of Computer Science
Vol 1, No 1, June 2007, pp 40-43
Faculty of Computer Science
ISSN 1994-6244

Upgrading Trust Factor Evaluation in AODV Protocol for MANET

Muhammad Ruhul Amin Khandaker[1], Md. Javed Kaiser[2],
Jugal Krishna Das[3] Md. Shahid Hossain[1] and Khandaker Razia Sultana[3]

ABSTRACT

In an ad hoc network, users communicate with each other from a temporary network, without any form of centralized administration. Each node participating in the network acts both as host and a router and must therefore be willing to forward packets for other nodes. The existing wireless routing protocols do not accommodate enough security for MANET and are highly vulnerable to attacks as malicious nodes may enter and leave the immediate radio transmission range at random intervals. To reduce this vulnerability and ensure security some researchers introduced trust levels of each node to select the neighbors. In this paper we introduce a technique for upgrading the trust levels of each node.

Key words: MANET, AODV, routing, secure neighbor, malicious node, trust factor/ level.

I. INTRODUCTION

Ad hoc network does not rely on any stationary infrastructure. The concept behind these infrastructures less networks is the collaboration between its participating members, i.e., instead of making data transit through a fixed base station, nodes consequentially forward data packets from one to another until a destination node is finally reached. Typically, a packet may travel through a number of network points before arriving at its destination. The operation of the system depends on distributed cooperation among all nodes in the network and fairly needs to trust the intermediate nodes between sender and receiver and the neighbors. Because of the improvised nature of ad-hoc networks, routes are built dynamically as and when nodes are regrouping (Discovery). Hence, ad hoc networks are more responsive to topology changing than any wired networks. Consequently, routing protocols for ad-hoc networks should be able to cope with link breakages and make sure that the network won't collapse as nodes are moving or shutting down. This paper describes secure neighbor detection for mobile ad hoc networks. In particular, we employ a trust-level based technique to find the nodes which might be neighbors for the ad hoc on-demand distance vector (AODV) routing protocol, a widely adopted ad hoc routing protocol. AODV is a reactive and stateless routing protocol that establishes routes only as desired by the source node. AODV is vulnerable to various kinds of attacks [15]. This paper analyzes some of the vulnerabilities, specifically discussing attacks against AODV that related to neighbors. We propose a solution based on the trust level to upgrade trust level as a malicious node may enter in network any time and ensue it cannot be chosen as the neighbor. The remainder of this paper is organized as follows: Section describes the secure neighbor in AODV. Section describes relative work on AODV security and intrusion detection on ad hoc networks. Section describes the upgrading technique of trust level in AODV. And finally in section we summarize the work

II. SECURE NEIGHBOR DETECTION IN AODV

Differentiating between a node and malicious in ad hoc networking environment is a challenging task. Malicious nodes may behave maliciously only erratically, further complicating their detection. A node that sends out false routing information could be the one that has been compromised, or merely one that has a temporarily stale routing table due to volatile physical conditions. Dynamic topologies make it difficult to obtain a global view of the network and any approximation can become quickly outdated. Therefore, secured neighbor detection is the first task for secured routing in AODV. In a network a node initiates path discovery process while it needs to communicate with another node if it does not have sufficient information. This process is accomplished by broadcasting a route request (RREQ) packet to its neighbor. After receiving a RREQ packet a node may reply back by forwarding RREP packet or rebroadcast RREQ to its neighbors. Before rebroadcast it will increase the hop field and remaining same the destination sequence number. The previous one is done if the receiving node is destination and the next one if it is an intermediate node. For a secured neighbor detection we propose to add several security modules with the existing AODV. In AODV protocol, a secure node wishing to communicate with a destination node, first broadcasts a RREQ packet to its neighbors. Upon receipt, the destination node reply RREP packet to the source. Each node maintains only the hop information to reach to destination. The route selection criteria of AODV based upon hop count and destination sequence number. Hop count determines how short the route is, and the sequence number of the

1. *Department of Computer Science and Engineering, IBAIS University, Dhaka Bangladesh.*
2. *Department of Computer Science and Engineering Northern University of Bangladesh, Dhaka Bangladesh.*
3. *Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka, Bangladesh.*

destination speaks about the freshness of the route information. Therefore, the route selection metric is clearly independent of the security level of the application and trust factor of the participating nodes.

Each node maintains a local database of its neighbors, where trust factor is dynamically updated 3]. Trust factor of each node calculated from the trust level is stored in the local database. Trust level of any node is defined from an integer value. Trust value is calculated from the activities of a node when routing occurs. Every node dynamically upgrades its trust level upon observing its neighbor.

This protocol allows both the initiator and target to verify that both are within their maximum transmission range. It is a simple three-round mutual authentication protocol. In 1st round, initiator sends a neighbor solicitation packet by. The target sends the reply by a solicitation packet after receiving the packet. In last round, the initiator sends neighbor verification, including broadcast authentication of a timestamp and the link from the source to destination. Now the total delay between these two subsequent messages is found by

$$\delta = t_1 - t_0.$$

The distance between them (with respect to initiator) is bounded by:

$$d <= \delta/2 * c,$$

where c is the speed of light in vacuum.

Thus, the initiator can check that the other party is within its maximum transmission range. The process of secure neighbor detection is performed off line.

Each node maintains a local database for maintaining a buffer with trust level of neighbor node. The following figure 1 shows the format of local database (with possible values):

Target Node	Packet ID <IP, Broadcast ID>	Forwarded (Y/N)	Unaltered (Y/N)
A	A, 0001	1	0

Figure 1: Format of the local database of each initiator node

III. RELATED WORKS

Yan et al. [16] proposed a trust model for secure routing evaluation in MANET. The authors defined a large trust evaluation matrix based on statistic data collected during the network communication. The statistic fields try to include different affective factors of the evaluation, such as pre-existing relationship among the nodes. A linear function is proposed to link these statistic fields together to compute the trust value about a certain node or nodes. However, no boundary evaluation value is defined in their approach. So it is difficult to define a threshold trust value for on-going tasks.

Virendra et al. [17] proposed a pair-wise trust evaluation scheme in MANETs. To evaluate the trustworthiness of a target node, a node implements some self evaluation on the target node while also considering other nodes' trust on the same target node. All trusts are evaluated via node monitoring on data delivery in the network. For computing self evaluation a traffic statistic function is mentioned, but not explicitly presented. To combine the self evaluation and others' trust, a relationship equation is defined. In the equation, self evaluation and others trust
are weighted with factor a1 and a2 respectively (a1+a2=1). The limitation of such relationship equation is that all different direct experiences are adjusted with one weight factor of same value.

It is evaluated two types of trust between a trustor node and a trustee node: *direct trust* and *recommendation trust*. Direct trust is a kind of credential gained by a trustor node through its direct experience upon the trustee node. Recommendation trust is the credential gained by a trustor node from a third node or nodes' recommendation on the trustee node.

Jugal Krishna Das, Shareeful Islam, Abu Raihan Mostofa Kamal, et al. 3] proposed a notation for calculating the trust factor as T [A , B, t] = x. It implies that the trust factor of a node A at time t is x measured by node B. Therefore it is a relative measure as T [A, B, t] ≠ T [A , B, t] is not a necessary condition. Trust factor of a node is determined by calculating the misbehaving of any node.

IV. A NEW MODEL FOR TRUST LEVEL MODIFICATION

A predefined time period t_m is set up and after the t_m time all entry of the local table will be deleted. A predefined threshold value $P_{threshold}$ is the determination parameter to detect a node as malicious. Our objective is to count the successful forwards by the target node. It can be easily computed by simply performing logical AND operation of the forward and reverse field of figure 2. Then the total number of 1s generates the desired successful packet forwards.

Target Node	Packet ID <IP, Broadcast ID>	Forwarded (Y/N)	Unaltered (Y/N)
A	A, 0001	0	0
A	A, 0002	1	0
A	A, 0003	1	1

A	A, 0004	1	0
A	A, 0005	1	1
A	A, 0006	1	1
A	A, 0007	1	1
A	A, 0008	1	1

Figure 2: Local database with assumed value

Suppose a snapshot for a period of t_m is generated by a node. Now by AND operation of the last two fields the resultant **transfer string** becomes **00101111.** So the number of the successful packet forwards

$$P_{success1} = 5$$

and the success factor ratio is

$$SFR_A = P_{success1} / P_{total}$$
$$= 5/8$$
$$=62.57\%.$$

Now D is calculated for a node A by subtracting the $P_{threshold}$ from the new calculated success factor ratio as

$$D = SFR_A - P_{threshold}$$

If $D \leq 0$ then the target node is detected as malicious. As each node maintains a local database of its neighbors with corresponding trust factor. So, the initiator updates the local database setting the trust factor of target node **–1**. The use of SFR1 instead of absolute number of successful packet forward $P_{success}$ has been carefully chosen.

Upgrade of trust factor mechanism is slightly different from that of degrade mechanism. But it uses almost the same algorithm for building the **transfer string**. Upgrade mechanism has two predefined values, t_t and $P_{threshold}$ which is necessarily equal values of t_m and $P_{threshold}$ respectively of the degrading process. The upgrading ratio will not be same as the degrading ratio. The value $P_{success2}$ is calculated by summing up the number of consecutive 1s from the LSB (Least Significant Bit). The SRF2 computation is similar to SRF1, and average the previous success ratio with the current success ratio.

$$SFR2 = \frac{P_{success2} / P_{total} + P_{success1}}{2}$$

Similarly, the degrading process D is calculated for a node A by subtracting the $P_{threshold}$ from the new calculated success factor ratio as

$$\mathbf{D = SFR_A - P_{threshold}}$$

If the If $D \geq 0$ then, the trust factor of the node is incremented by 1. If SRF2 exceeds $P_{threshold}$ but does not exceed by predefined value then trust factor is not incremented.

Hence, notation for calculating the trust factor is

$$T[A, B, t, f] = x$$

For secured routing, we want to ensure that a malicious node can not be trusted by evaluating once. If its consecutive success ratio is satisfactory only then it is trusted as a secured neighbor [detection is more essential.] Hence, the upgrading is slower than degrading. A node, which is not malicious may have suffered by this technique.

The above notation implies that the trust factor of a node A at time t with previous success ratio f is x measured by node B.

V. CONCLUSION

In this paper, we proposed a trust factor upgrading technique of nodes in MANET. Here, both pre-existing knowledge and direct interaction among nodes in the network can be taken into account. In our scheme, upgrading technique may not allow a secured neighbor at the first time when route is discovered as its previous trust level will be zero. But it ensures that no malicious node entering in a network will be trusted. As the next step of developing a general trust model, we plan to extend our trust model to a general form to overcome this problem and we will also look further at some issues like avoiding count to infinity problem.

VI. REFERENCE

[01] C. Perkins and E. Belding-Royer and S. Das, 2002. "Ad hoc On-Demand Distance Vector (AODV) Routing ", *RFC 3561*, July 2003.

[02] Qifeng Lu, Dec 15, 2002. "Vulnerability of Wireless Routing Protocols".

[03] Jugal Krishna Das, Shareeful Islam and Abu Raihan Mostofa Kamal, "An analysis and solution of security vulnerability of AODV routing protocol in Mobile Ad Hoc Networks".

[04] Lyes Guemari, August 20, 2001. "An OPNET model implementation for Ad-hoc On demand Distance Vector Routing Protocol".

[05] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer, Richard A. Kemmerer, 2004. "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks".

[06] Tony Larson, Nicklas Hedman, 1998. "Routing Protocols in Wireless Ad-hoc Networks- A Simulation Study".

[07] Ian D. Chakeres, Elizabeth M. Belding-Royer. "AODV Routing Protocol Implementation Design ".

[08] Nikola Milanovic, Miroslaw Malek, Anthony Davidson, Veljko Milutinovic. "Routing and Security in Mobile Ad Hoc Networks".

[09] Karl Levitt. "Intrusion Detection for Mobile Ad Hoc Networks—Internet".
[10] Charles E perkins, 2001. "Ad hoc Networking".
[11] Peng Ning, Kun Sun, 2003. "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Adhoc Routing Protocols," in Proceedings of the 4th Annual *IEEE Information Assurance Workshop*, pages 60-67, West Point, June 2003.
[12] Stephen Carter, Alec Yasinsac. "Source Position Aided Ad Hoc Routing".
[13] Kwan-Wu Chin, John Judge, Aidan Williams and Roger Kermode. "Implementation Experience with MANET Routing Protocols".
[14] L. Zhou, and Z. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no.6, Nov/Dec 1999.
[15] Mohamed M. Abou El Saoud. "MANET reference configurations and evaluation of service location protocol for MANET".
[16] Yan, Z., P. Zhang, and T. Virtanen. "Trust Evaluation Based Security Solution in Ad Hoc Networks" in Proceedings of the Seventh Nordic Workshop on Secure IT Systems 2003. 2003. Norway.
[17] Virendra, M., et al. "Quantifying Trust in Mobile Ad-Hoc Networks" in International Con-ference on Integration of Knowledge Intensive Multi-Agent Systems, 2005 (KIMAS '05). 2005. Waltham, Massachusetts, USA: IEEE.